SPYWOLF

Security Audit Report

Audit prepared for

Monstro's Degenz V1.5

Completed on

February 11, 2024

SPYWOLF.CO

@SPYWOLFNETWORK

@SPYWOLFNETWORK

OVERVIEW

This goal of this report is to review the main aspects of the project to help investors make an informative decision during their research process.

You will find a a summarized review of the following key points:

- ✓ Contract's source code
- ✓ Owners' wallets
- ✓ Tokenomics
- ✓ Team transparency and goals
- ✓ Website's age, code, security and UX
- ✓ Whitepaper and roadmap
- ✓ Social media & online presence

> *The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal*
>
> - SPYWOLF Team -

KEY RESULTS

Cannot mint new tokens	N/A
Cannot pause trading (honeypot)	*
Cannot blacklist an address	Passed
Cannot raise taxes over 25%?	Passed
No proxy contract detected	Passed
Not required to enable trading	*
No hidden ownership	Passed
Cannot change the router	N/A
No cooldown feature found	Passed
Bot protection delay is lower than 5 blocks	N/A
Cannot set max tx amount below 0.05% of total supply	Passed
The contract cannot be self-destructed by owner	Passed

N/A = Not applicable for this type of contract

*Only new deposits/reinvestments can be paused

For a more detailed and thorough examination of the heightened risks, refer to the subsequent parts of the report.

TABLE OF CONTENTS

Monstro's Degenz V1.5

PROJECT DESCRIPTION

According to their whitepaper:
"Are you a DeFi enthusiast who loves the allure of profitable ROI dApps but hates enduring endless losses? Look no further than Monstro's Degenz! Unleash your inner degen amongst the safety of your fellow monsters."

Release Date: Launching Feb 14, 2024

Category: ROI dApp, Farming

CONTRACT INFO

Token Name MonstroDegenzS1v2	Symbol N/A
Contract Address Not Deployed	
Network N/A	Language Solidity
Deployment Date Not Deployed	Contract Type Staking
Total Supply N/A	Status Not Deployed

TAXES

Buy Tax
***30% + ref reward**

Sell Tax
5%

***Distribution of buy tax according to the project's team: "Farmz working capital, which benefits the user as it is their "safety net" passive income for when the "ROI dApp" phase runs dry." Referral reward tax can be up to 20%, depending on referral's cashback settings.**

For more information check their documents page:
https://wiki.monstro.fun/universe/

Our Contract Review Process

The contract review process pays special attention to the following:

- ✓ Testing the smart contracts against both common and uncommon vulnerabilities
- ✓ Assessing the codebase to ensure compliance with current best practices and industry standards.
- ✓ Ensuring contract logic meets the specifications and intentions of the client.
- ✓ Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- ✓ Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

TOKEN TRANSFERS STATS

Transfer Count	N/A
Uniq Senders	N/A
Uniq Receivers	N/A
Total Amount	N/A
Median Transfer Amount	N/A
Average Transfer Amount	N/A
First transfer date	N/A
Last transfer date	N/A
Days token transferred	N/A

SMART CONTRACT STATS

Calls Count	N/A
External calls	N/A
Internal calls	N/A
Transactions count	N/A
Uniq Callers	N/A
Days contract called	N/A
Last transaction time	N/A
Created	N/A
Create TX	N/A
Creator	N/A

VULNERABILITY ANALYSIS

ID	Title	
SWC-100	Function Default Visibility	Passed
SWC-101	Integer Overflow and Underflow	Passed
SWC-102	Outdated Compiler Version	Passed
SWC-103	Floating Pragma	Passed
SWC-104	Unchecked Call Return Value	Passed
SWC-105	Unprotected Ether Withdrawal	Passed
SWC-106	Unprotected SELFDESTRUCT Instruction	Passed
SWC-107	Reentrancy	Passed
SWC-108	State Variable Default Visibility	Passed
SWC-109	Uninitialized Storage Pointer	Passed
SWC-110	Assert Violation	Passed
SWC-111	Use of Deprecated Solidity Functions	Passed
SWC-112	Delegatecall to Untrusted Callee	Passed
SWC-113	DoS with Failed Call	Passed
SWC-114	Transaction Order Dependence	Passed
SWC-115	Authorization through tx.origin	Passed
SWC-116	Block values as a proxy for time	Passed
SWC-117	Signature Malleability	Passed
SWC-118	Incorrect Constructor Name	Passed

VULNERABILITY ANALYSIS

ID	Title	
SWC-119	Shadowing State Variables	Passed
SWC-120	Weak Sources of Randomness from Chain Attributes	Passed
SWC-121	Missing Protection against Signature Replay Attacks	Passed
SWC-122	Lack of Proper Signature Verification	Passed
SWC-123	Requirement Violation	Passed
SWC-124	Write to Arbitrary Storage Location	Passed
SWC-125	Incorrect Inheritance Order	Passed
SWC-126	Insufficient Gas Griefing	Passed
SWC-127	Arbitrary Jump with Function Type Variable	Passed
SWC-128	DoS With Block Gas Limit	Passed
SWC-129	Typographical Error	Passed
SWC-130	Right-To-Left-Override control character (U+202E)	Passed
SWC-131	Presence of unused variables	Passed
SWC-132	Unexpected Ether balance	Passed
SWC-133	Hash Collisions With Multiple Variable Length Arguments	Passed
SWC-134	Message call with hardcoded gas amount	Passed
SWC-135	Code With No Effects	Passed
SWC-136	Unencrypted Private Data On-Chain	Passed

THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

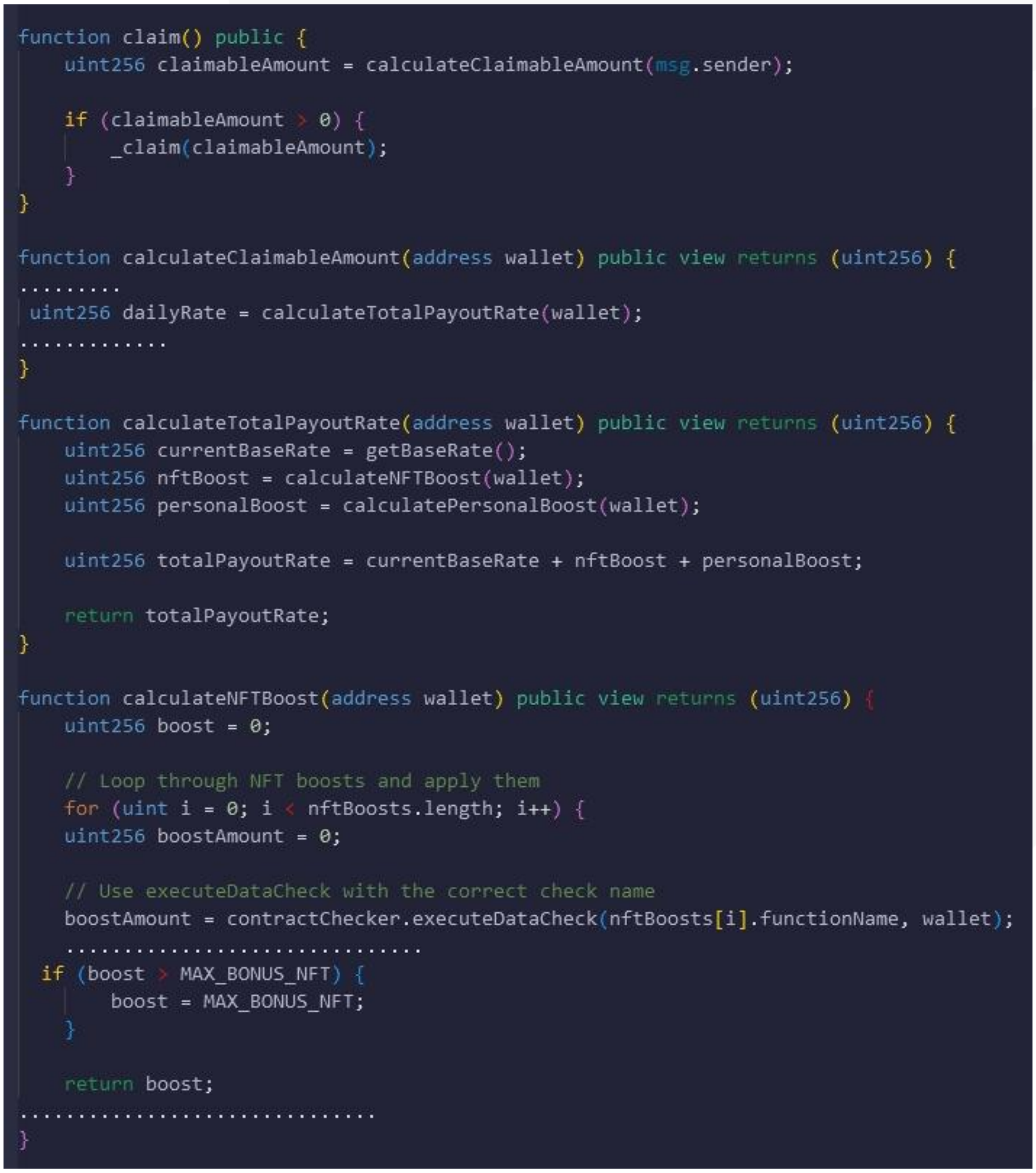
Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

FOUND THREATS

⚠ Medium Risk

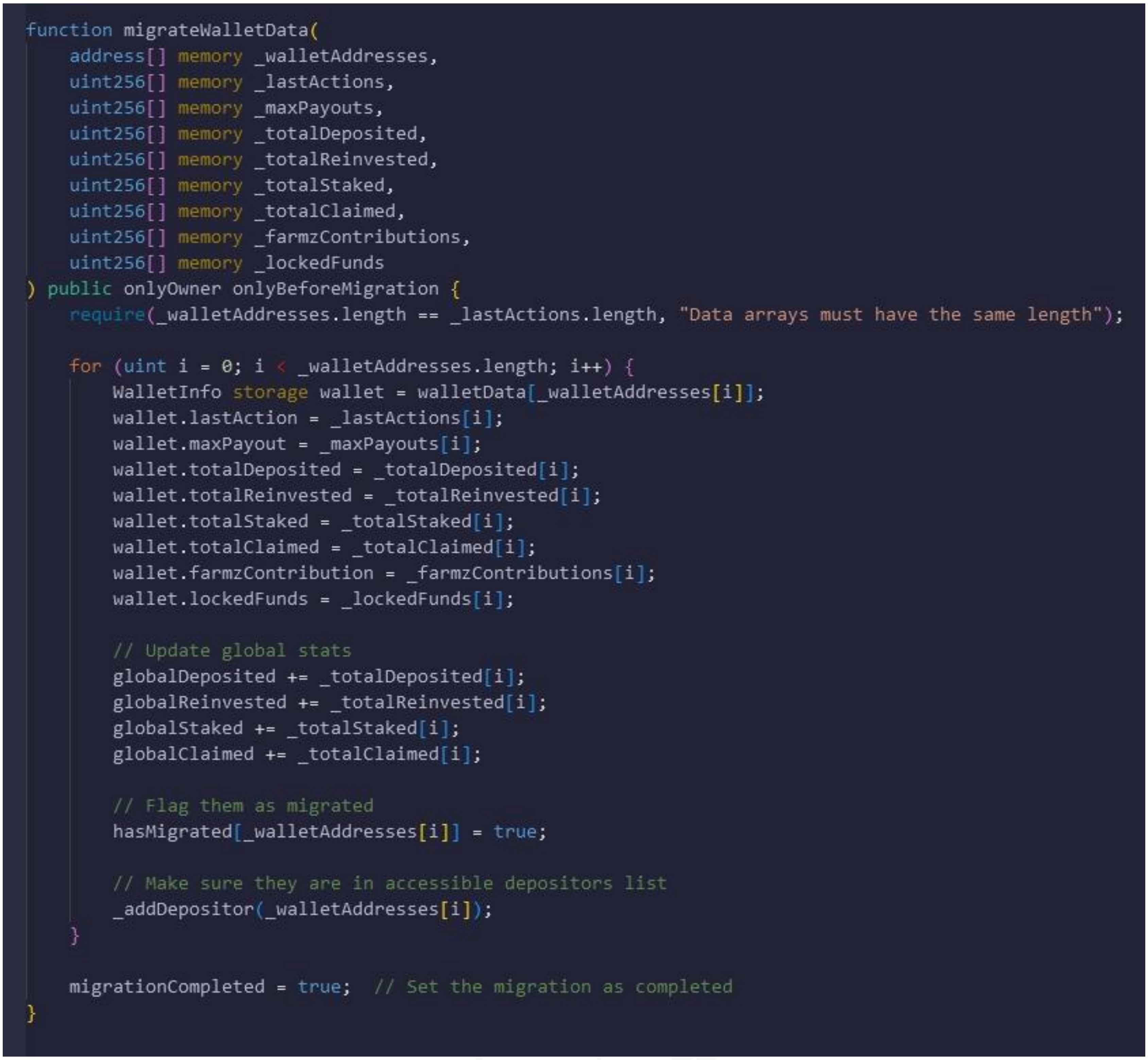
Payout calculating function uses external contract to check user.
If the external contract return incorrect data and/or halt on function call, the current claim() function will also halt.
The external contract may return max nft boost (1%) to selected users.



```
function claim() public {
    uint256 claimableAmount = calculateClaimableAmount(msg.sender);

    if (claimableAmount > 0) {
        _claim(claimableAmount);
    }
}

function calculateClaimableAmount(address wallet) public view returns (uint256) {
.........
 uint256 dailyRate = calculateTotalPayoutRate(wallet);
.............
}

function calculateTotalPayoutRate(address wallet) public view returns (uint256) {
    uint256 currentBaseRate = getBaseRate();
    uint256 nftBoost = calculateNFTBoost(wallet);
    uint256 personalBoost = calculatePersonalBoost(wallet);

    uint256 totalPayoutRate = currentBaseRate + nftBoost + personalBoost;

    return totalPayoutRate;
}

function calculateNFTBoost(address wallet) public view returns (uint256) {
    uint256 boost = 0;

    // Loop through NFT boosts and apply them
    for (uint i = 0; i < nftBoosts.length; i++) {
    uint256 boostAmount = 0;

    // Use executeDataCheck with the correct check name
    boostAmount = contractChecker.executeDataCheck(nftBoosts[i].functionName, wallet);
    ...............................
  if (boost > MAX_BONUS_NFT) {
        boost = MAX_BONUS_NFT;
    }

    return boost;
...............................
}
```

Informational

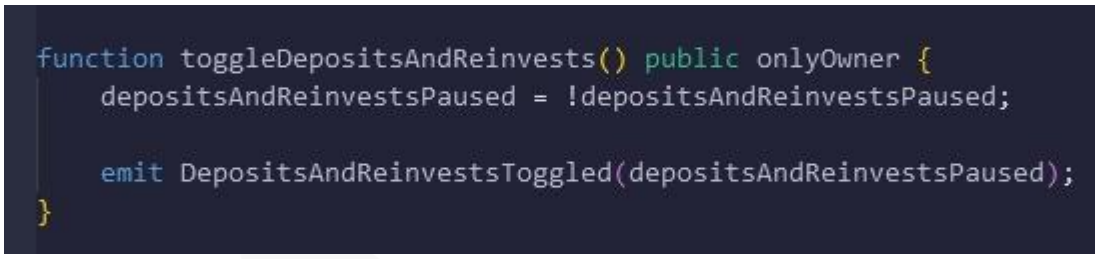
Owner can migrate users with manually filled data only once.



```
function migrateWalletData(
    address[] memory _walletAddresses,
    uint256[] memory _lastActions,
    uint256[] memory _maxPayouts,
    uint256[] memory _totalDeposited,
    uint256[] memory _totalReinvested,
    uint256[] memory _totalStaked,
    uint256[] memory _totalClaimed,
    uint256[] memory _farmzContributions,
    uint256[] memory _lockedFunds
) public onlyOwner onlyBeforeMigration {
    require(_walletAddresses.length == _lastActions.length, "Data arrays must have the same length");

    for (uint i = 0; i < _walletAddresses.length; i++) {
        WalletInfo storage wallet = walletData[_walletAddresses[i]];
        wallet.lastAction = _lastActions[i];
        wallet.maxPayout = _maxPayouts[i];
        wallet.totalDeposited = _totalDeposited[i];
        wallet.totalReinvested = _totalReinvested[i];
        wallet.totalStaked = _totalStaked[i];
        wallet.totalClaimed = _totalClaimed[i];
        wallet.farmzContribution = _farmzContributions[i];
        wallet.lockedFunds = _lockedFunds[i];

        // Update global stats
        globalDeposited += _totalDeposited[i];
        globalReinvested += _totalReinvested[i];
        globalStaked += _totalStaked[i];
        globalClaimed += _totalClaimed[i];

        // Flag them as migrated
        hasMigrated[_walletAddresses[i]] = true;

        // Make sure they are in accessible depositors list
        _addDepositor(_walletAddresses[i]);
    }

    migrationCompleted = true;  // Set the migration as completed
}
```

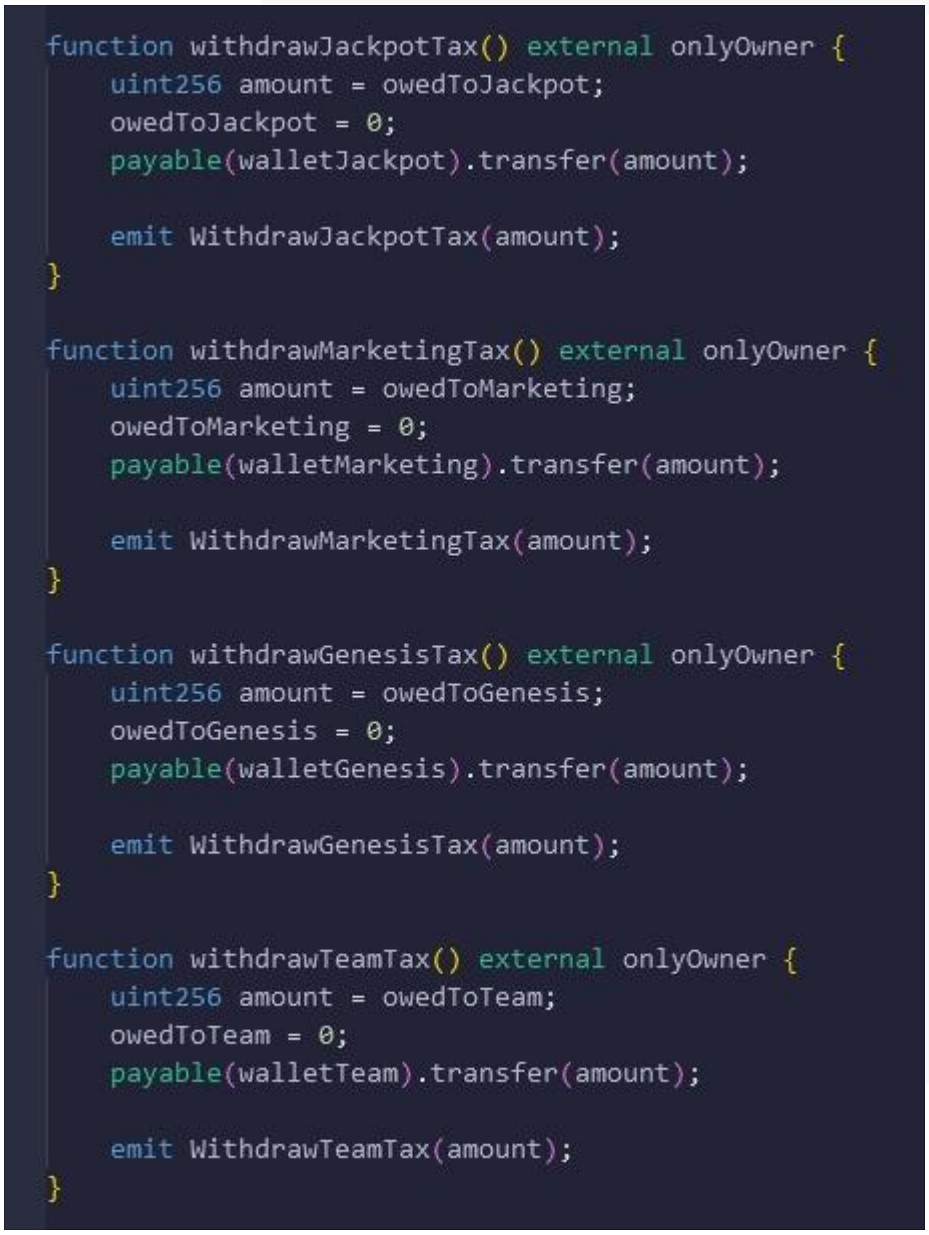
Informational

Owner can pause new deposits and reinvestments.



```
function toggleDepositsAndReinvests() public onlyOwner {
    depositsAndReinvestsPaused = !depositsAndReinvestsPaused;

    emit DepositsAndReinvestsToggled(depositsAndReinvestsPaused);
}
```

Owner can withdraw bnb from the contract for amounts up to the taxes collected for team/marketing/jacpot/genesis.

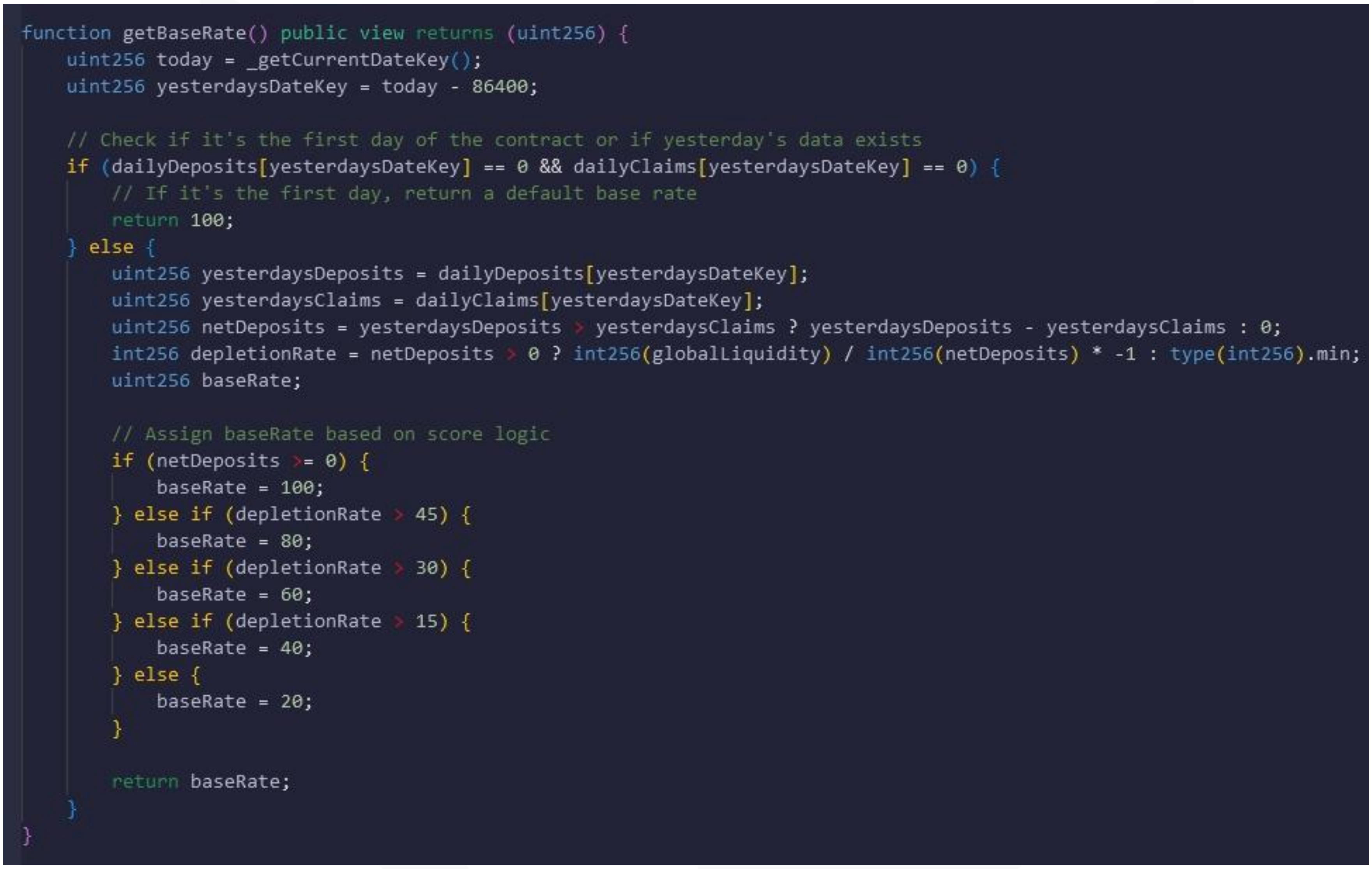


```
function withdrawJackpotTax() external onlyOwner {
    uint256 amount = owedToJackpot;
    owedToJackpot = 0;
    payable(walletJackpot).transfer(amount);

    emit WithdrawJackpotTax(amount);
}

function withdrawMarketingTax() external onlyOwner {
    uint256 amount = owedToMarketing;
    owedToMarketing = 0;
    payable(walletMarketing).transfer(amount);

    emit WithdrawMarketingTax(amount);
}

function withdrawGenesisTax() external onlyOwner {
    uint256 amount = owedToGenesis;
    owedToGenesis = 0;
    payable(walletGenesis).transfer(amount);

    emit WithdrawGenesisTax(amount);
}

function withdrawTeamTax() external onlyOwner {
    uint256 amount = owedToTeam;
    owedToTeam = 0;
    payable(walletTeam).transfer(amount);

    emit WithdrawTeamTax(amount);
}
```

Informational

baseRate will always be 100 as netDeposits will always be greater or equal to 0.

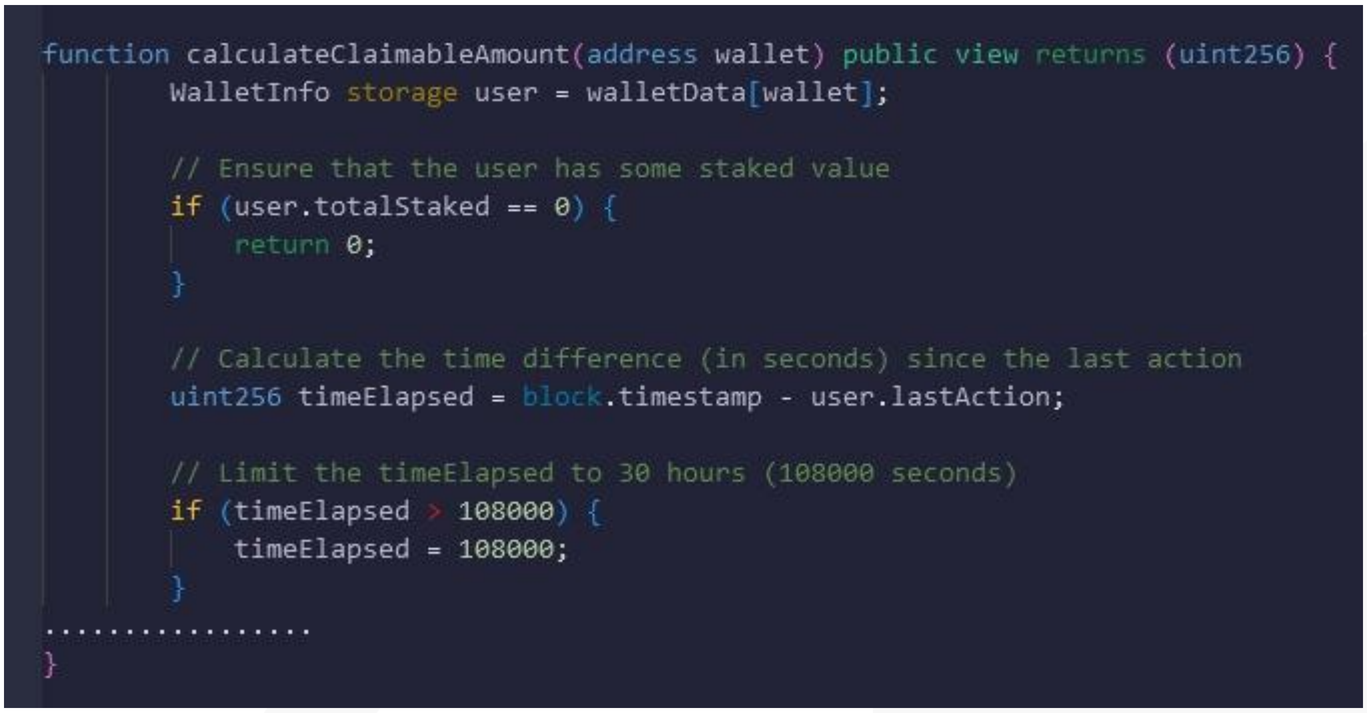
depletionRate will always return negative number and negative numbers will be always less than 45, 30 and 15.



```
function getBaseRate() public view returns (uint256) {
    uint256 today = _getCurrentDateKey();
    uint256 yesterdaysDateKey = today - 86400;

    // Check if it's the first day of the contract or if yesterday's data exists
    if (dailyDeposits[yesterdaysDateKey] == 0 && dailyClaims[yesterdaysDateKey] == 0) {
        // If it's the first day, return a default base rate
        return 100;
    } else {
        uint256 yesterdaysDeposits = dailyDeposits[yesterdaysDateKey];
        uint256 yesterdaysClaims = dailyClaims[yesterdaysDateKey];
        uint256 netDeposits = yesterdaysDeposits > yesterdaysClaims ? yesterdaysDeposits - yesterdaysClaims : 0;
        int256 depletionRate = netDeposits > 0 ? int256(globalLiquidity) / int256(netDeposits) * -1 : type(int256).min;
        uint256 baseRate;

        // Assign baseRate based on score logic
        if (netDeposits >= 0) {
            baseRate = 100;
        } else if (depletionRate > 45) {
            baseRate = 80;
        } else if (depletionRate > 30) {
            baseRate = 60;
        } else if (depletionRate > 15) {
            baseRate = 40;
        } else {
            baseRate = 20;
        }

        return baseRate;
    }
}
```

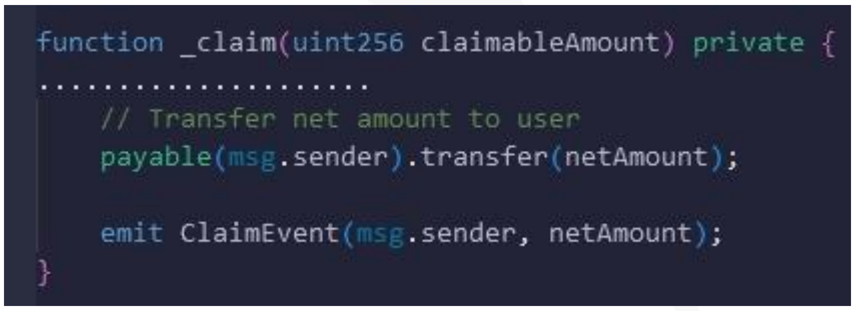
Informational

There is a 30 hours cutoff period for staking rewards.
Example - User stake and want to claim their rewards after 4 days, he/she will get the rewards for 30 hours period but not for 4 days.



```
function calculateClaimableAmount(address wallet) public view returns (uint256) {
        WalletInfo storage user = walletData[wallet];

        // Ensure that the user has some staked value
        if (user.totalStaked == 0) {
            return 0;
        }

        // Calculate the time difference (in seconds) since the last action
        uint256 timeElapsed = block.timestamp - user.lastAction;

        // Limit the timeElapsed to 30 hours (108000 seconds)
        if (timeElapsed > 108000) {
            timeElapsed = 108000;
        }
.................
}
```

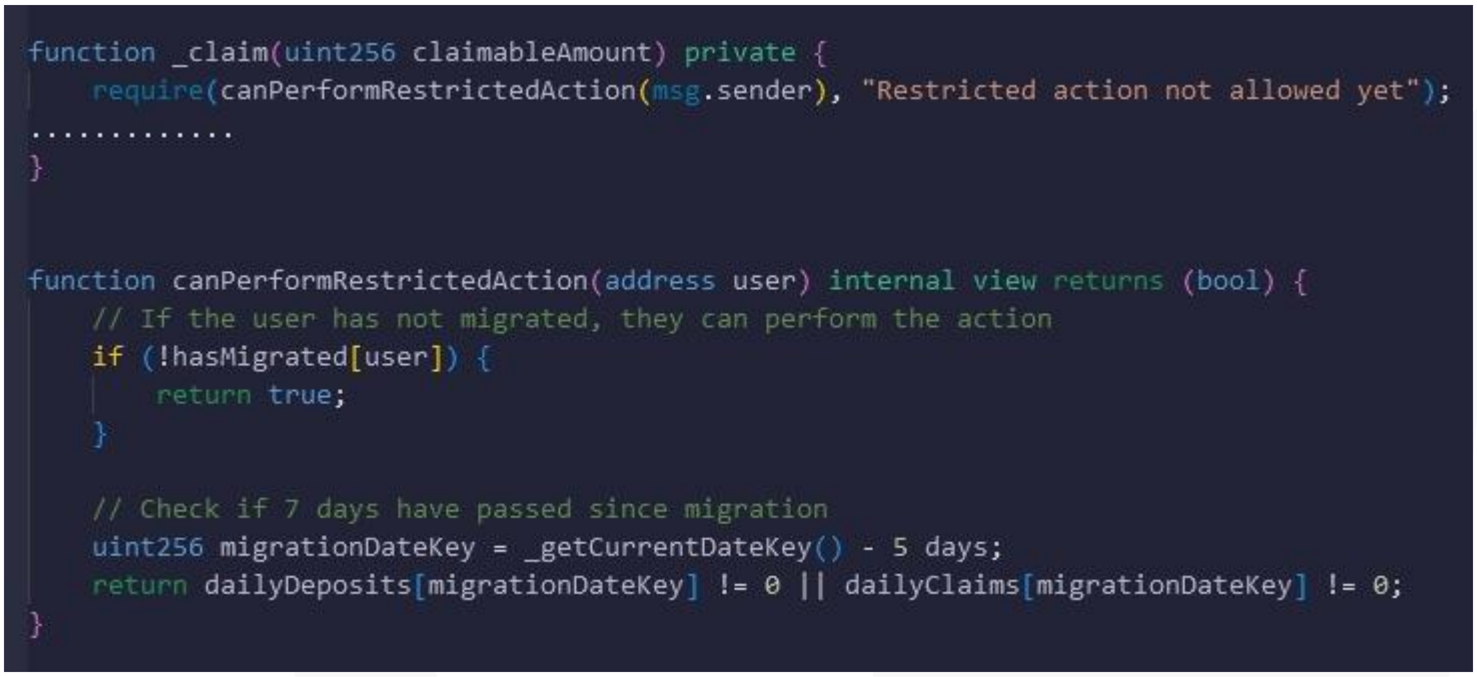
Some multisig wallets and/or another wallets in form of contracts might not claim rewards from the staking as only 2300 gas is reserved for the transfer.
This is valid only if the transfer changes states in the receiving contract and if the receiving contract cannot receive ether.



```
function _claim(uint256 claimableAmount) private {
.....................
    // Transfer net amount to user
    payable(msg.sender).transfer(netAmount);

    emit ClaimEvent(msg.sender, netAmount);
}
```

Informational

Migrated users can claim rewards at least after 6 days after migration is done.



```
function _claim(uint256 claimableAmount) private {
    require(canPerformRestrictedAction(msg.sender), "Restricted action not allowed yet");
.............
}


function canPerformRestrictedAction(address user) internal view returns (bool) {
    // If the user has not migrated, they can perform the action
    if (!hasMigrated[user]) {
        return true;
    }

    // Check if 7 days have passed since migration
    uint256 migrationDateKey = _getCurrentDateKey() - 5 days;
    return dailyDeposits[migrationDateKey] != 0 || dailyClaims[migrationDateKey] != 0;
}
```

RECOMMENDATIONS FOR

GOOD PRACTICES

1. Consider fundamental tradeoffs
2. Be attentive to blockchain properties
3. Ensure careful rollouts
4. Keep contracts simple
5. Stay up to date and track development

Monstro's Degenz

GOOD PRACTICES FOUND

✓ The owner cannot set a transaction limit

TOKENOMICS

This is a ROI contract offering daily ROI up to 3%
Users can increase their daily ROI through NFT and Personal "boosts". NFT bonuses are up to 1% and deposit value bonuses up to 1% allow for a total of 3% daily ROI.

Deposited funds are allocated as follows:
65% - Liquidity
30% - Farmz
5% - Marketing

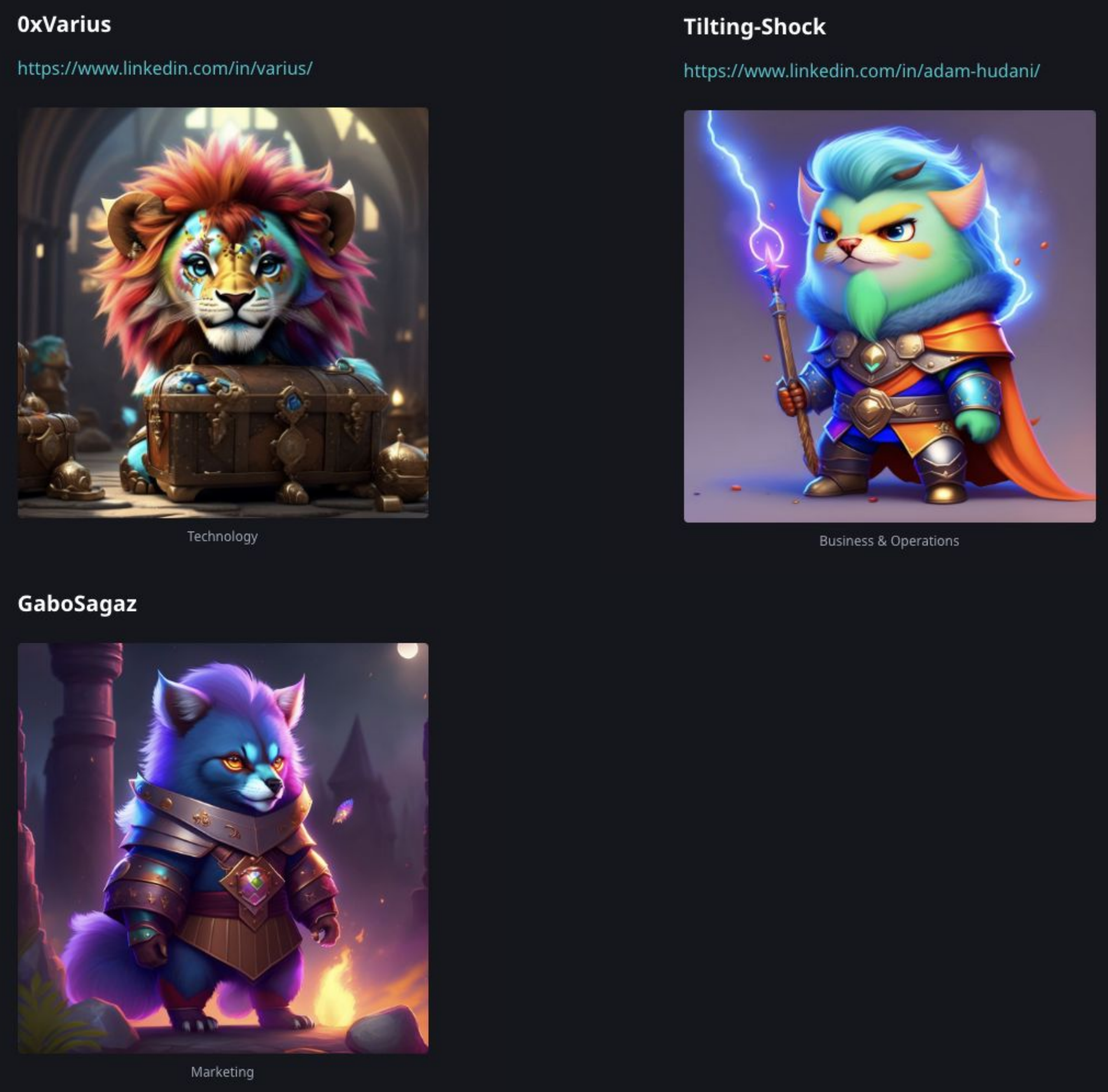
Claims are subject to a 10% tax:
4% - Team
2.5% - Jackpot
2.5% - Marketing
1% - Genesis NFT holders

**ROI* - Return of investment*

ROI dapps are usually subject to high volatility and considered as high risk investments.

THE TEAM

✅ The team at Monstro is well-known and publicly doxxed. Linkedin profiles were provided.



0xVarius

https://www.linkedin.com/in/varius/

Technology

Tilting-Shock

https://www.linkedin.com/in/adam-hudani/

Business & Operations

GaboSagaz

Marketing

WEBSITE

Home Website URL
https://monstro.fun/

Domain Registry
https://namecheap.com

Domain Expiration
2024-04-20

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

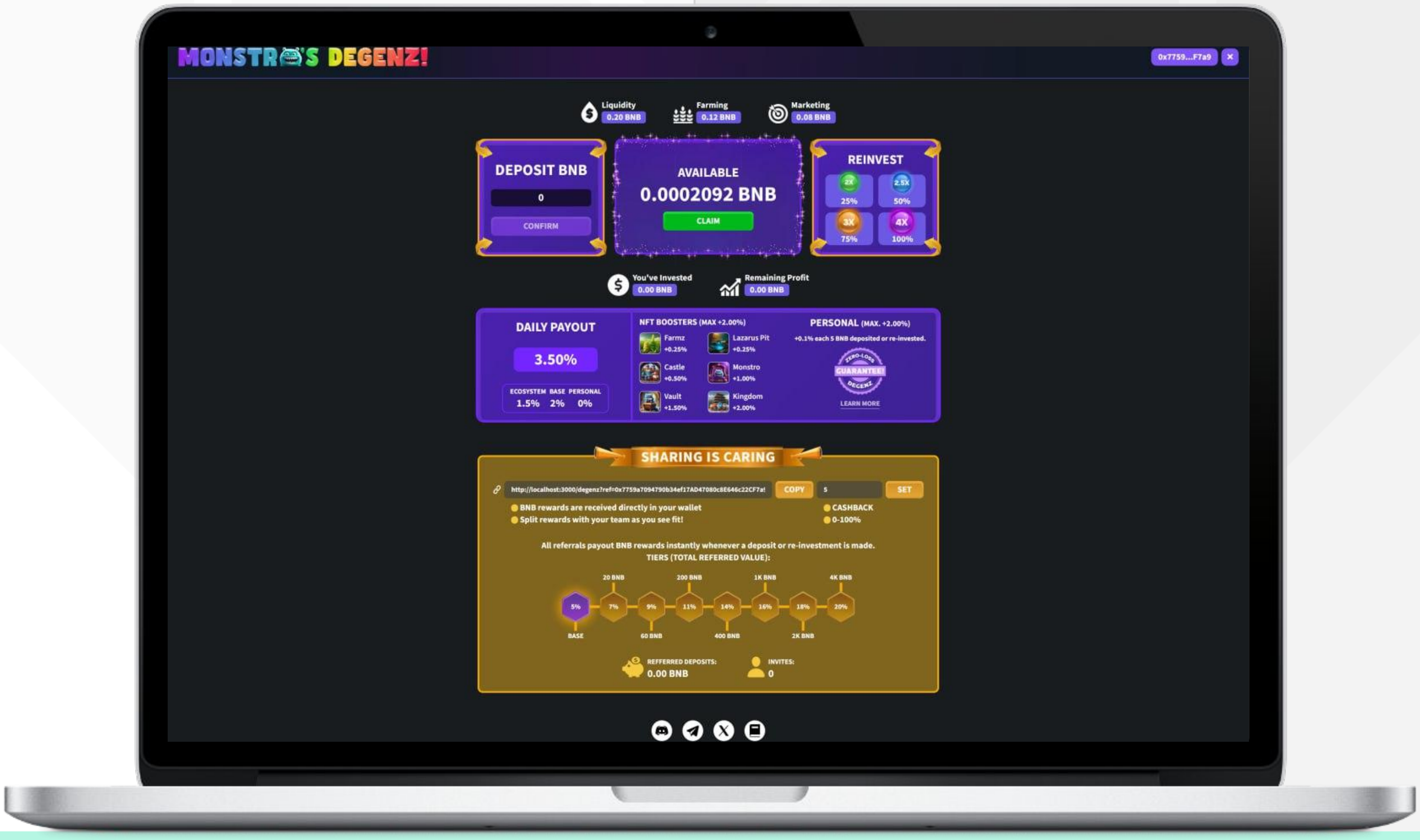
Design
Very nice color scheme and overall layout.

Content
The information helps new investors understand what the product does right away. No grammar mistakes found.

Whitepaper
Well written and explanatory documents page

Roadmap
Yes, goals set

Mobile-friendly?
Yes



Liquidity 0.20 BNB

Farming 0.12 BNB

Marketing 0.08 BNB

0

0.0002092 BNB

You've Invested 0.00 BNB

Remaining Profit 0.00 BNB

DAILY PAYOUT 3.50%

ECOSYSTEM	BASE	PERSONAL
1.5%	2%	0%

NFT BOOSTERS (MAX +2.00%)

Farmz +0.25%	Lazarus Pit +0.25%
Castle +0.50%	Monstro +1.00%
Vault +1.50%	Kingdom +2.00%

PERSONAL (MAX. +2.00%)

+0.1% each 5 BNB deposited or re-invested.

http://localhost:3000/degenz?ref=0x7759a7094790b34ef17AD47080c8E646c22CF7a!

5

- BNB rewards are received directly in your wallet
- Split rewards with your team as you see fit!

- CASHBACK
- 0-100%

All referrals payout BNB rewards instantly whenever a deposit or re-investment is made.

TIERS (TOTAL REFERRED VALUE):

REFFERRED DEPOSITS: 0.00 BNB

INVITES: 0

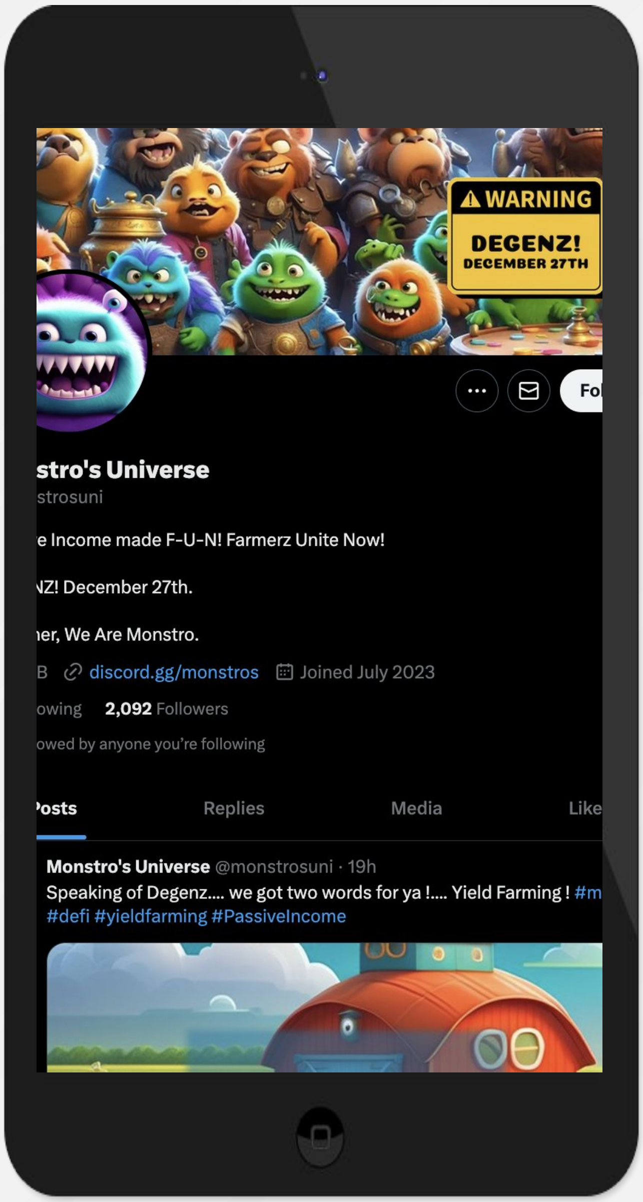
monstro.fun/degenz

SOCIAL MEDIA

& ONLINE PRESENCE

ANALYSIS

Project’s social media pages are very active with devs and users interacting often.



stro's Universe
strosuni

e Income made F-U-N! Farmerz Unite Now!

NZ! December 27th.

ner, We Are Monstro.

B discord.gg/monstros Joined July 2023

owing 2,092 Followers

owed by anyone you’re following

Monstro's Universe @monstrosuni · 19h
Speaking of Degenz.... we got two words for ya !.... Yield Farming ! #m
#defi #yieldfarming #PassiveIncome

Twitter

@monstrosuni

- 2 092 followers
- Active
- Posts frequently

Discord

@monstros

- 1718 members
- Active community

Telegram

@monstrosU

- 980 members
- Active members
- Active mods

Medium

- Not available

SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- ✓ OVER 700 SUCCESSFUL CLIENTS
- ✓ MORE THAN 1000 SCAMS EXPOSED
- ✓ MILLIONS SAVED IN POTENTIAL FRAUD
- ✓ PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS
- ✓ CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE

SPYWOLF.CO

@SPYWOLFNETWORK

@SPYWOLFNETWORK

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.

While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:

By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.

No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.

The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.

No applications were reviewed for security. No product code has been reviewed.